WAVESTONE

Industrial sites cybersecurity

Benchmark on 40 assessments

Wavestone

We support large companies and organizations in their most critical transformations.

Business & technology

12 offices
in 8 countries

Turnover
422 M€

+3 500
employees

Cybersecurity & Digital Trust

+500 consultants
+1000 missions per year

Speakers

Gérome Billois

gerome.billois@wavestone.com

Arnaud Soullié

arnaud.soullie@wavestone.com

Alexandrine Torrents

alexandrine.torrents@wavestone.com

Introduction

MAKE THE 4TH INDUSTRIAL REVOLUTION A REALITY

WAVESTONE

A dedicated team to support the industrial CISO, maintain security over time and prepare plants for cyber crises.

US | UK | FR | BE | CH | LU | HK

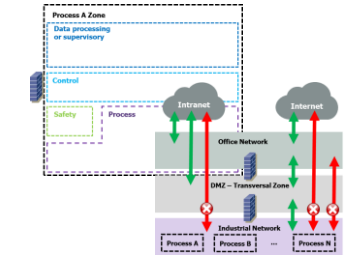
INDUSTRIAL CYBERSECURITY STRATEGY

- Target Operating Model & Governance
- Strategy & Roadmap and Budget Definition
- Cyber assessment and risk analysis

Hands-on approach and toolkit

SECURE-BY-DESIGN INDUSTRY 4.0

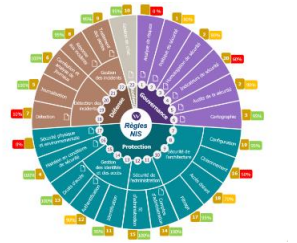
- Build a secure industrial network
- Enforce PLC, SCADA… protection
- Deploy security solutions



Security models

INDUSTRIAL CONTROL SYSTEMS ASSESSMENT

- Organizational and physical assessment
- Architecture and configuration review
- Penetration testing



Evaluation system

Industrial sites cybersecurity benchmark

OT cybersecurity benchmark

~40

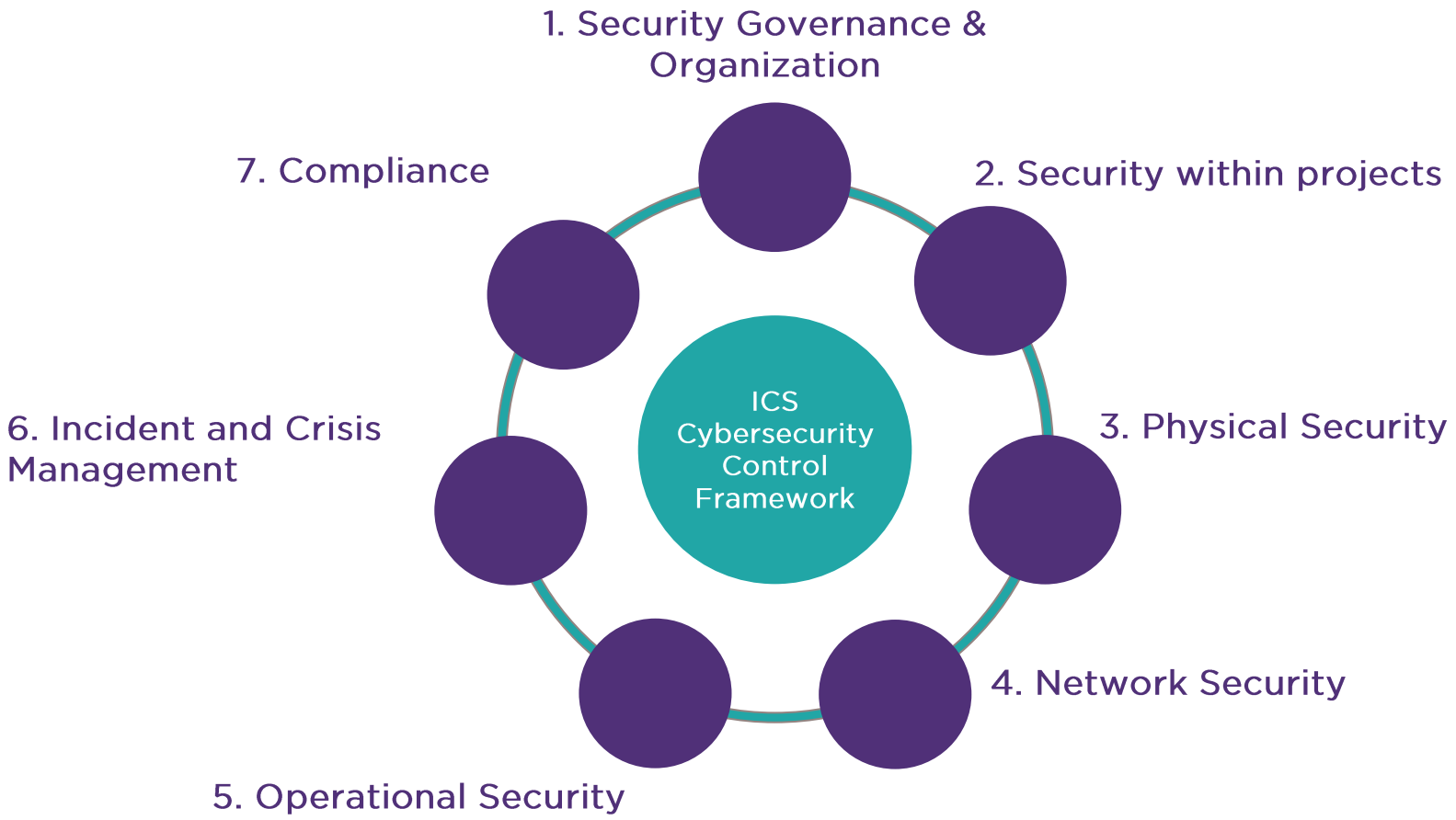
Industrial sites considered in this benchmark, assessed in 2019 & 2020

~10

Clients concerned in a wide range of sectors (pharmaceutical, energy, water cycle, spirits, agri-food, etc.)

Our assessment methodology

Wavestone has developed an **industrial site assessment framework**, adaptable to the **specificities of the sector or the client**, allowing a global assessment of the cybersecurity level of a site or a production line



Focus on 5 key themes

Focus on 5 key themes

Governance

Network segmentation

Remote access

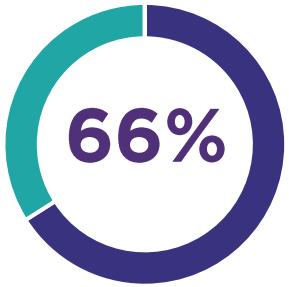
System administration

Resilience

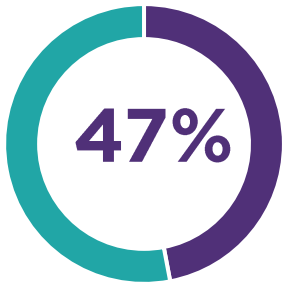
Governance

Who's in charge of ICS cybersecurity?

A specific ICS policy exists



An on-site cybersecurity manager is identified



Cyber requirements for 3rd parties are defined

Governance is a key issue, which tends to be overlooked in cybersecurity projects.

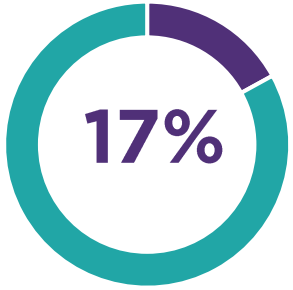
It is necessary to create mixed IT/OT teams, and the support of IT cybersecurity teams is generally necessary for the upskilling of OT teams.

Although dedicated cybersecurity tools can help in improving the level of security, no tool will replace qualified personnel.

Network segmentation

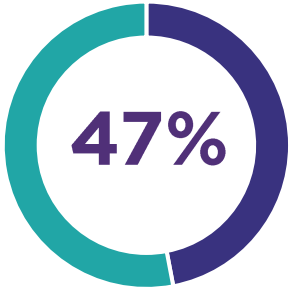
No ICS is 100% isolated.

PLCs on the office network



PLCs accessible from the office network

Presence of a DMZ between IT & OT



Network segmentation is often a good starting point for ICS security projects.

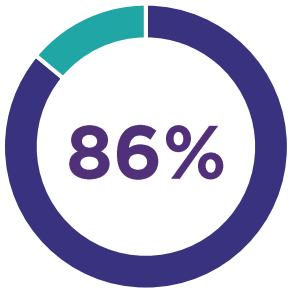
Safety Instrumented Systems are the most sensitive assets to protect and should be segmented first.

A network segmentation project usually involves other technical (Active Directory) and organizational (RACI for system administration) segmentation projects.

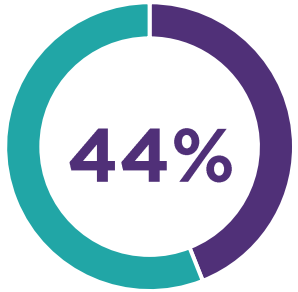
Remote access

Remote access is a business need.

Remote access to ICS exists



There is a site-to-site connection between the ICS and a third party



Use of unofficial solutions for remote access

It is very common for part of the industrial perimeter to be under the responsibility of third parties, often requiring remote access for maintenance or even supervision.

It is recommended to provide a vetted solution to avoid insecure local initiatives.

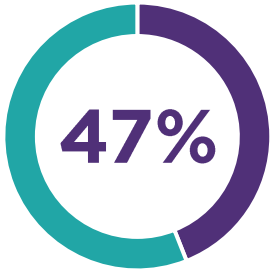
It is important to take into account the specific needs of the sites (real-time monitoring of third party actions by a local actor, non-permanent and limited access to certain machines) when defining the proposed solution.

System administration

Segmentation is not just a network issue.

No security patches applied

No AV/EDR solution



Windows OT machines are part of the corporate AD

The system administration of standard equipment (Windows type) requires specific skills and appropriate training, both of which are rarely present on the OT side.

The application of security patches is necessary, but should be done in a pragmatic way, based on the exposure of the equipment. Over-investment in the subject should be avoided.

As long as OT equipment is part of the corporate Active Directory, an attacker or ransomware can propagate to the ICS, regardless of the network filtering rules.

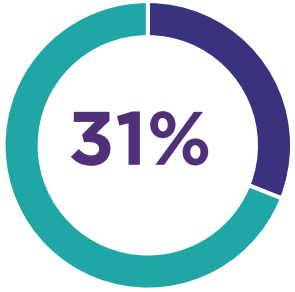
Resilience

Think resilience globally.

Suffered a production-impacting incident within 12 months

Use of obsolete components without sufficient/controlled spare parts

The site has an up-to-date inventory



Although backups are usually present, it is rare that they cover all the machines needed for production, especially machines provided and managed by a third party.

It is essential to have a detailed and up-to-date view of your equipment, and to integrate elements supplied by & under the responsibility of third parties (packaged PLCs / blackbox).

For many industries, especially manufacturing, the availability of production lines is not sufficient for resilience, other systems need to be integrated into the overall thinking (MES, ERP...).

Rethinking the vision of OT

The traditional vision

Why is OT security 20 years behind?

Very long-life components (+20 years), frequent obsolescence

The main criterion is availability, not confidentiality

Recent use of standard components & protocols

Systems designed to be isolated but now connected

The new vision

Leveraging the strengths of OT

Few changes once the system is secured

No data encryption issues

Quality culture & good change management

Dedicated safety systems to prevent a major incident

ICS operations = Safety **+** Availability **+** Quality

OT cybersecurity, why be interested in it?

IT/OT convergence

Use of IT systems for industrial process monitoring and control

1

Increased connectivity

With third parties: predictive maintenance, analytics

With office systems: use of MES, exchange with ERP, production of KPIs...

2

Arrival of standard IT components, protocols and techniques

(MQTT, Single Pair Ethernet, virtualization)

3

Soft-PLCs !

Even elements very close to the physical process are beginning to be standardized or even virtualized

How to start your industrial site security project?

STEP 1

Knowing your ICS & industrial processes

STEP 2

Limiting network exposure

STEP 3

Pragmatic view of security patches

STEP 4

Ensuring end-to-end resilience

Put the human at the center of the cybersecurity approach

Start small & grow

Authors

Arnaud Soullié
Manager

arnaud.soullie@wavestone.com

Manager in Cybersecurity and Digital Trust at Wavestone, Arnaud conducts security audits and penetration tests, now specializing in ICS cybersecurity . He speaks at conferences such as BlackHat EU, DEFCON or BruCOn. He also created DYODE, an open-source network diode.

Alexandrine Torrents
Senior Consultant

alexandrine.torrents@wavestone.com

Alexandrine is specialized in auditing and penetration testing, with a focus on industrial IS security, and assists major accounts in bringing their installations into compliance with French (LPM) and European (NIS) regulations. She is ISA/IEC 62443 certified.